Public-Key Cryptography and Message Authentication

Dr. Bhaskar Mondal

Public-Key Cryptography Principles

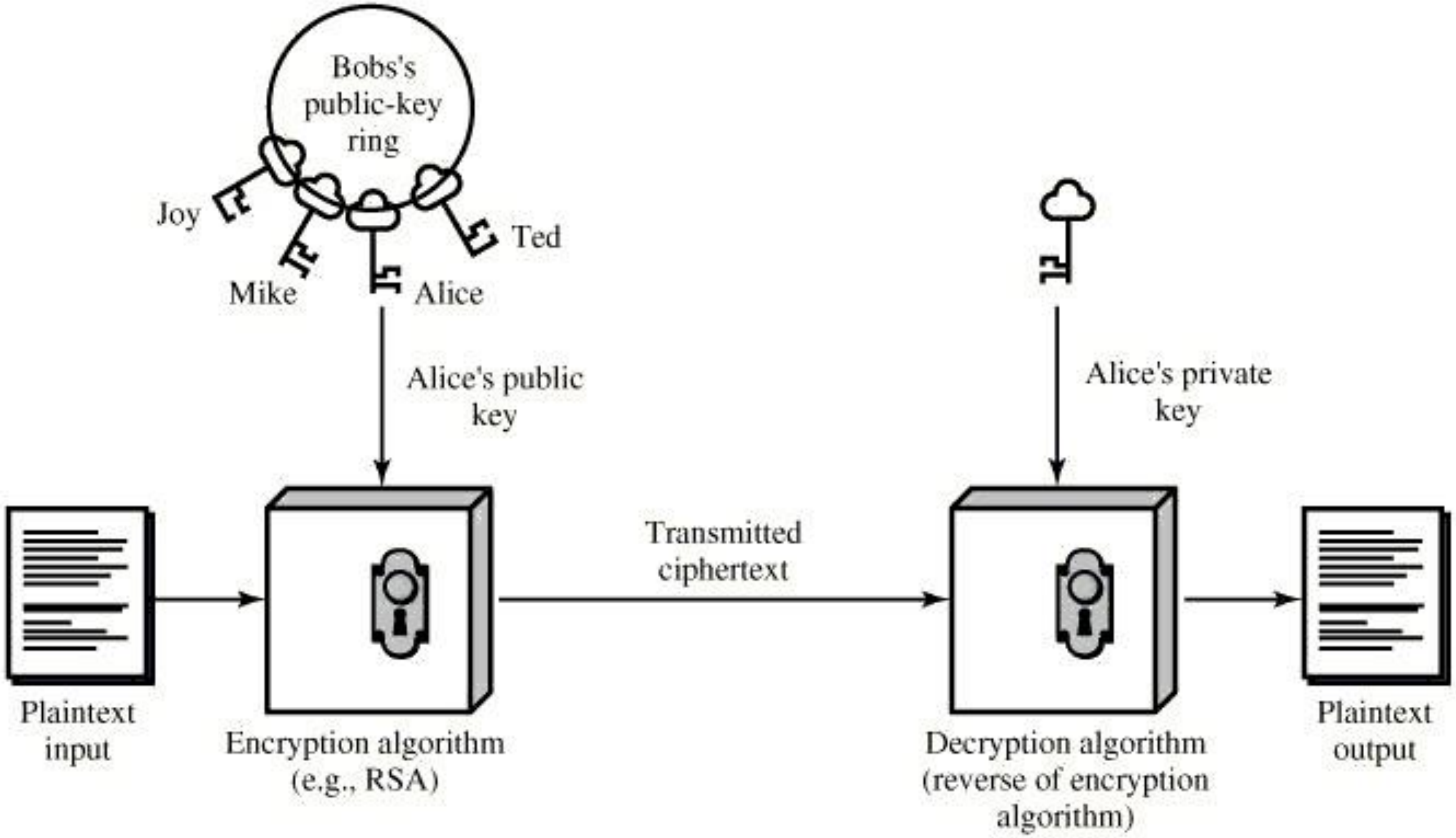
The use of two keys has consequences in: key distribution, confidentiality and authentication.

The scheme has six ingredients

- Plaintext
- Encryption algorithm
- Public and private key
- Ciphertext
- Decryption algorithm

- Public key like Bank Account Number and Private key is like a PIN

Encryption using Public-Key system



(a) Encryption

Authentication using Public-Key System

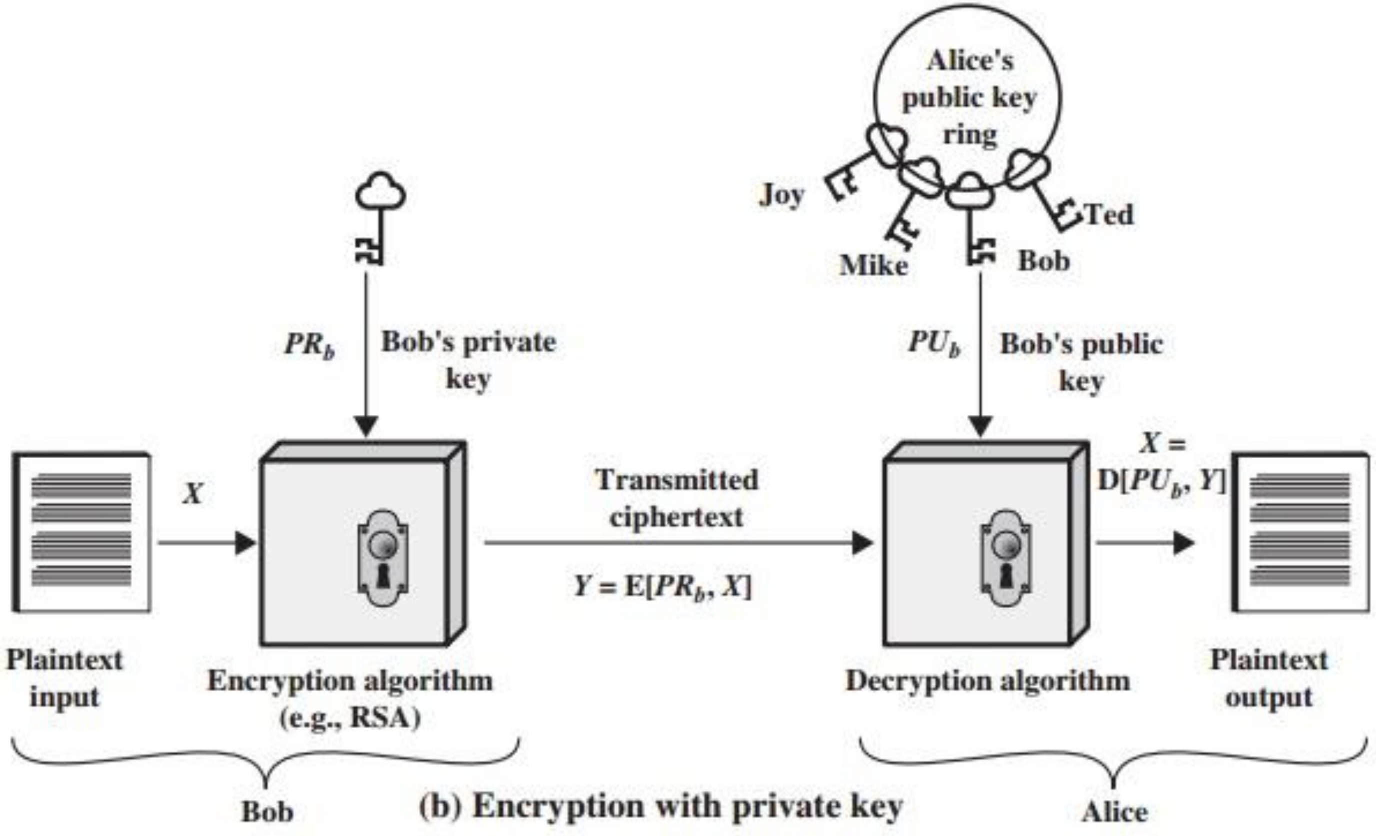


Figure 9.1 Public-Key Cryptography

Applications for Public-Key Cryptosystems

Encryption/decryption

Digital signature

Key echange

Requirements for Public-Key Cryptography

- Computationally easy for a party B to generate a pair (public key KUb, private key KR_b)
- Easy for sender to generate ciphertext:
- Easy for the receiver to decrypt ciphertect using private key:

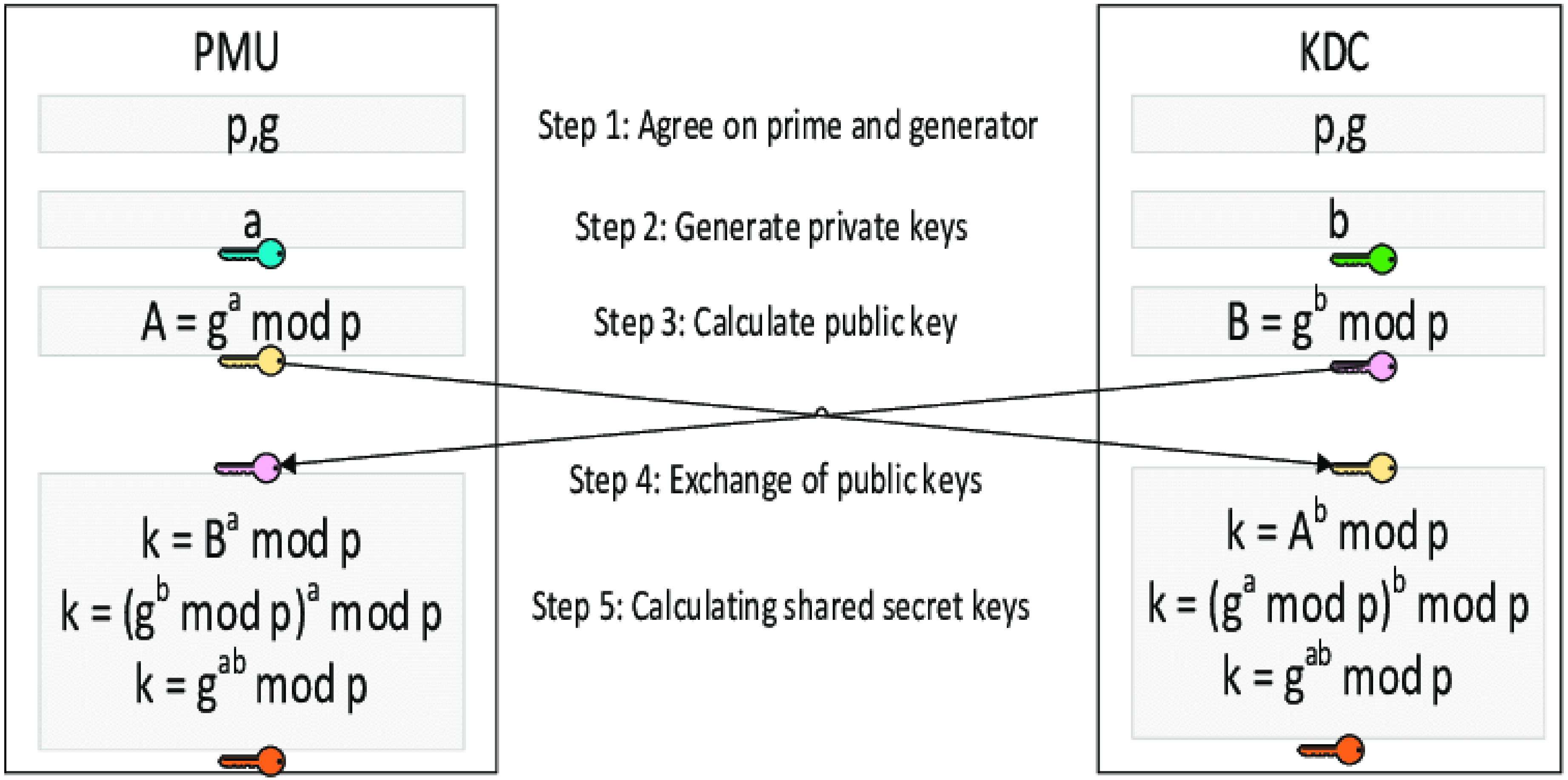
$$C = E_{KUb}(M)$$

$$M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$$

Public-Key Cryptographic Algorithms

RSA	Diffie-Hellman	Digital Signature Standard (DSS)	Elliptic-Curve Cryptography (ECC)
• Integer factoring • Key sharing		• Makes use of the SHA-1 • Not for encryption or key echange	• Good for smaller bit size • Low confidence level, compared with RSA • Very complex

Diffie-Hellman Key Exchange



Example

Step 1

Alice and Bob get public numbers

P = 23,

G = 9

Step 2

Alice selected a private key

a = 4 and

Bob selected a private key b = 3

Step 3

Alice and Bob compute public values

- Alice:

x =(9^4 mod 23) = (6561 mod 23) = 6

- Bob:

y = (9^3 mod 23) = (729 mod 23) = 16

Step 4

Alice and Bob exchange public numbers

Step 5

Alice receives public key y =16 and

- Bob receives public key

x = 6

Step 6

Alice and Bob compute symmetric keys

- Alice:

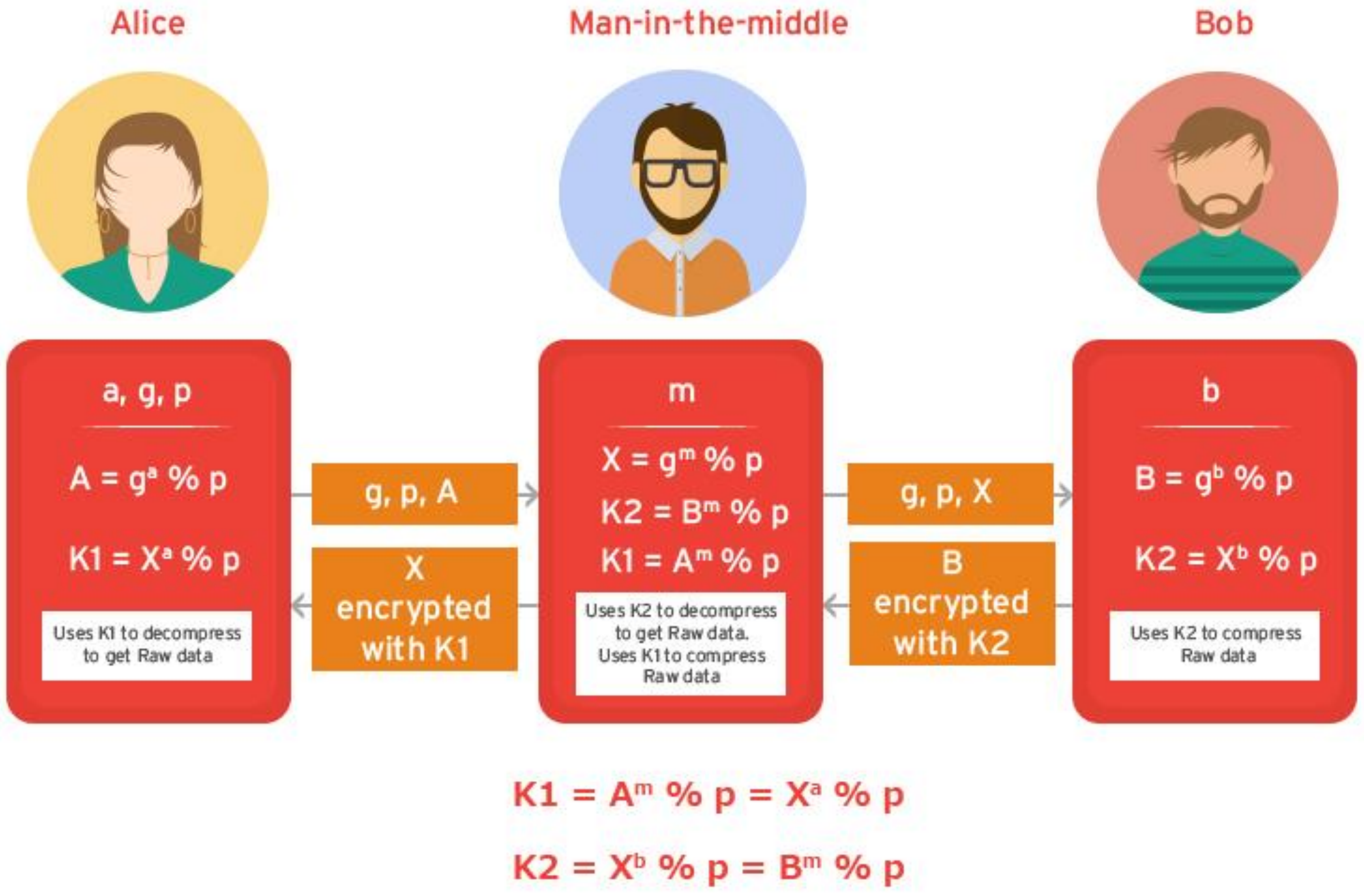
ka = y^a mod p = 65536 mod 23 = 9

- Bob:

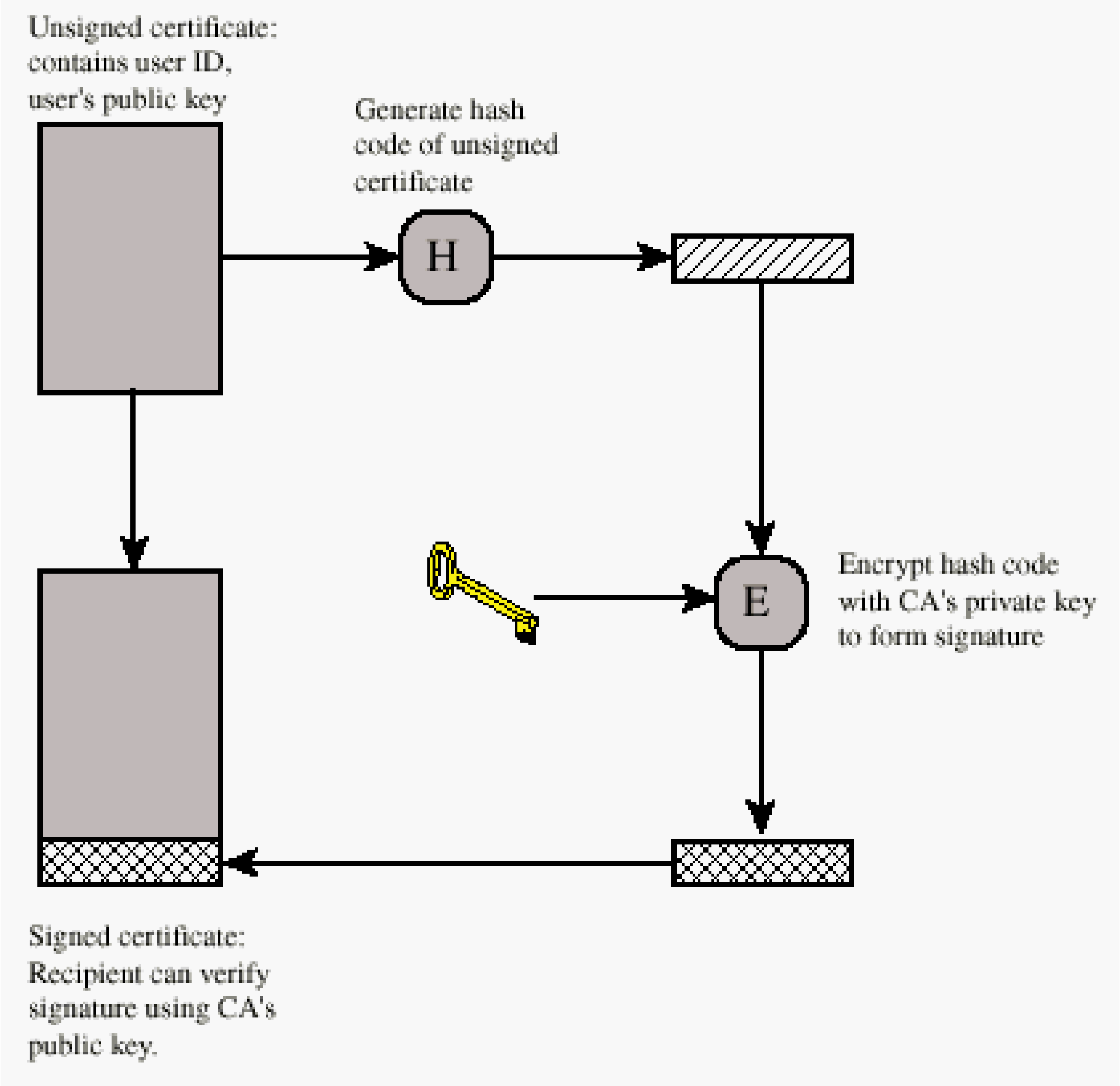
kb = x^b mod p = 216 mod 23 = 9

Step 7

is the shared secret.



Diffie-Hellman Key Exchange



Key Management Public-Key Certificate Use

Message Security Requirements (attacks)

- Disclosure
- Traffic analysis
- Masquerade
- Content modification
- Sequence modification
- Timing modification
- Source repudiation
- Destination repudiation

Approaches to Message Authentication

Authentication Using Conventional Encryption	Message Authentication without Message Encryption	Message Authentication Code
• Only the sender and receiver should share a key	• An authentication tag is generated and appended to each message	• Calculate the MAC as a function of the message and the key. $MAC = F(K, M)$

MAC Authentication

- concerned of message origin authentication, not confidentiality.
- symmetric key cryptographic technique
- sender and receiver share a symmetric key K.
- MAC is an encrypted checksum generated
- Similar to hash, fixed length output.

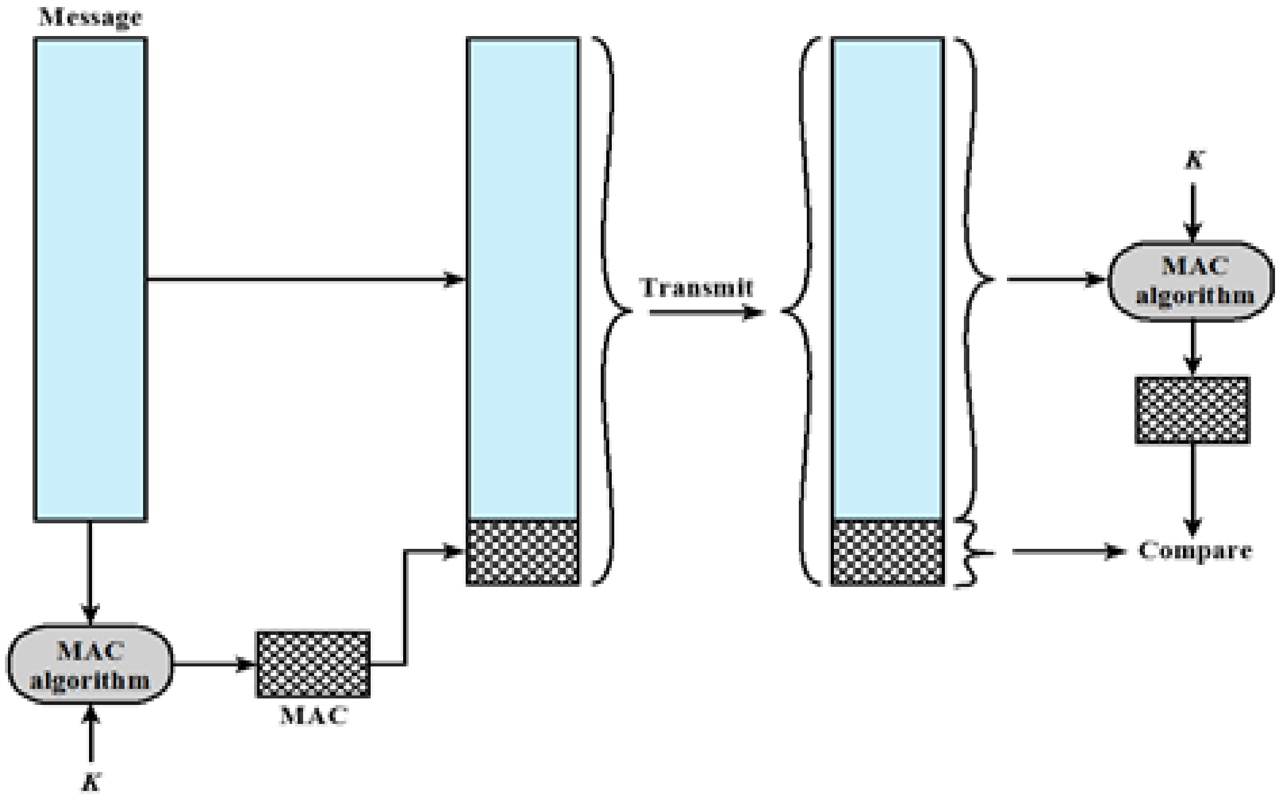


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).

References

- William Stallings, Network Security Essentials : Applications and Standards, ISBN: 9788131761755, 8131761754

- Thanks to the many unknown sources from where some information is adopted.